УДК 658.7

CRM 系统的销售转化策略研究

刘俊杰 (Liu Junjie)
白俄罗斯国立大学商学院
e-mail: 1695383617@qq.com

Summary. *In the era of rapid development of digital economy, more and more enterprises are beginning to use digital technology to carry out marketing business. As one of the important resources of enterprises, customer relationship management system (CRM) plays a very critical role in the daily operation of enterprises.*

本文以客户关系管理系统为例，从线索获取、识别、培育、转化四个角度去探讨系统中销售转化存在的问题。

1.研究意义

数字信息化时代，企业更多的开始选择借助数字化信息平台来开展市场营销业务，客户关系管理系统（CRM）也在最近几年受到企业市场的青睐。市面上做 CRM 软件服务的 SAAS 公司有很多，但因为企业的差异性和独特性是不可避免的，所以出现企业业务和所使用的 CRM 系统配对的功效发挥不足。而对于企业来讲，一个适合公司的 CRM 可以为企业创造巨大的利润。

2.系统中销售转化过程存在的问题

目前线索获取阶段存在的问题包括获取销售线索的途径还比较保守、线索质量比较差 [0]。线索识别阶段识别效率低、没有对线索价值进行有效划分。线索培育阶段沉默线索没有激活、触达行为效果差。线索转化阶段转化率低等问题，导致销售的沉默线索沉积，销售也无法激活行动，遗失潜在的商机。

3. 客户关系管理系统改进建议

线索获取改进建议：获客渠道优化，在互联网场景化下，线上流量是当下企业所要争取的。同时利用分销策略可以采取全员分销的策略，为公司内部人员开通分销账号，通过二级分销返利，为企业创造利润，带来新客户；

线索识别改进建议：通过设计线索的清洗规则，查重规则设定好后，可以设计触达条件或者做定时清洗任务，系统自动清洗线索。评级策略，通过开发自定义线索评级模板，规定分值，启用后系统则根据参数规则进线评级。

线索培育改进建议：线索池管理，必须备注无效原因，以免线索资源浪费。精细化触达，从以上这些问题，我们可以找出两个关键点：底层数据的建立、系统的自动化配置。激活沉默的线索，可进行人工建立系统自动化触达流程。

线索转化改进建议：优化线索流转机制，通过在系统中建立不同的客户池，来保障线索流动，确保线索的价值和有效；利用数据分析线索转化情况，建立可视化图表,可清晰的通过实际数据来表现数据流转问题，提高转化率。

综上所述：对于 CRM 的建设，可以先从企业的战略层去考虑，CRM 的定位决定其延展性功能结构。从企业发展的长远角度去看待 CRM 的建设，既要做到不画蛇添足，也要从业务的延展性考虑功能的兼容性。

参考文献

1. 杨路明,杨竹青,谢伊苹.客户关系管理理论与实务[M].北京:电子工业出版社，2015:35-41.

2. Kubina M, Lendel V. Successful application of social CRM in the company [J]. – Procedia Economics and Finance, 2015. – 23(10). – P. 1190–1194.

УДК 658.7

A STUDY OF THE SET MEMBER FILTERING PROBLEM CONSIDERING NETWORK ATTACKS

马世宽 (Ma Shikuan), 尚书旗 (Shang Shuqi), 何晓宁 (He Xiaoning), 崔孟君 (Cui Mengjun)

青岛农业大学 (Qingdao Agricultural University)

e-mail: woshimashikuan@163.com

Summary. *In recent years, set member filtering has received extensive research interest due to its engineering significance of estimating sets that contain the true state of the system rather than individual vectors. More importantly, communication protocols are widely used in control systems for their ability to prevent data conflicts and reduce network burden. This paper provides an overview of how to model and how to deal with the situation of being under cyber-attack in a networked control system (NCS).*

The security of networked control systems is an important issue to be considered, and cyber-attacks are widely found in communication networks, as shown in figures 1 and 2, which can degrade the performance of networked systems or even destroy them. Especially for wireless sensor networks, network attacks propagate between sensor nodes along the network topology and greatly damage the performance of wireless sensor networks. Therefore, there is an urgent need to consider security under network attacks in wireless sensor networks.